UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/824,132	04/03/2001	Mark M. Stephenson	00479.00001	8931

22907 7590 01/03/2006

BANNER & WITCOFF
1001 G STREET N W
SUITE 1100
WASHINGTON, DC 20001

EXAMINER	
BHATIA, AJAY M	
ART UNIT	**PAPER NUMBER**
2145	

DATE MAILED: 01/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/824,132	STEPHENSON ET AL.	
	Examiner	Art Unit	
	Ajay M. Bhatia	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-13,15,19-22,24,26-32,34-38 and 45-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-13,15,19-22,24,26-32,34-38 and 45-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/24/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

Applicant's arguments with respect to claims 1-56 have been considered but are moot in view of the new ground(s) of rejection. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.

Applicant may wish to contact examiner for interview before responding to this action about possible amendments.

Also examiner is sorry about any confusion about the status of the cause, applicant was correct that the prior action was a final rejection. Examiner will look into the issues with Pair and hope will try to resolve them to prevent this from this confusion to the applicant.

Also examiner has returned the 1449, IDS.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4-5, 7-8, 11-13, 15, 19-22, 24, 26-56 rejected under 35 U.S.C. 103(a) as being unpatentable over TunnelBuilder for Mac User's Guide (referred to as MacTB) in view of TunnelBuilder 4.01 for Windows Website (referred to as WinTB).

For claim 1, MacTB teaches, a system for establishing communications across a firewall comprising:

a communications network; (MacTB, Chapter 1, private lan)

a first server within said communications network; (MacTB, Chapter 1, company lan, pptp/l2tp server)

a first computer separated from said communications network, said first computer sending information to said first server; and, (MacTB, Chapter 1, remote location, company network)

a second computer separated from said communications network, said second computer receiving information from said first server related to the information sent from said first computer, (MacTB, Chapter 1, it is a message from one computer to another)

wherein at least one of said first computer and said second computer are separated from said communications network by at least one firewall. ((blah), Chapter 1, remote location, company network, firewall)

wherein said first computer transmits a hypertext transfer protocol (HTTP) message to said first server with an encrypted identification of said second computer, (MacTB, Chapter 1, 1st remote computer, 2nd PPTP/L2TP, Internet message is HTTP)

wherein said first server decrypts said encrypted identification to an unencrypted identification of said second computer and forwards said message to said second computer using said unencrypted identification, (MacTB, Chapter 1, PPTP/L2TP server unencrypts)

MacTB fails to clearly disclose, wherein said HTTP message is transmitted through a firewall port that is normally open by default to Internet traffic

WinTB teaches, wherein said HTTP message is transmitted through a firewall port that is normally open by default to Internet traffic (see applicant's specification "generally open" in paragraph 4 of the specification) (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80)

It would have been obvious to on of ordinary skill in the art at the time of the invention was made to combine the features of MacTB with WinTB because they are both made by the same company have a program with more advanced feature makes it more profitable, if it is available on all patforms.

For claim 2, MacTB teaches, the system according to claim 1, wherein said first computer transmits a said message to said first server with encrypted message content and said server transmits said encrypted content to said second computer without

decrypting said message in said server. (MacTB, Chapter 1, inherent to sending traffic over the internet, the intermediate server that route the packet will do so based on the outer packet of the encapsulated pack, very similar to the Russian dolls that are nest within each other, you can only see the out side part till it open the doll within it is taken out)

For claim 4, MacTB-WinTB teaches, the system according to claim 1, wherein said first computer further includes a first client and said second computer includes a second client and wherein each of said first client and said second client use an open firewall port that is normally open by default to Internet traffic to access said communications network. (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) (see applicant's specification "generally open" in paragraph 4 of the specification)The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 4.

For claim 5, MacTB-WinTB teaches, the system according to claim 4, wherein said open port is at least one of port 80 and port 8080. (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 5.

For claim 7, MacTB teaches, the system according to claim 1, wherein the information received at said second computer has the same content as the information sent from said first computer. (MacTB, Chapter 1, see page 1-1, the encapsulated message)

For claim 8, MacTB teaches, the system according to claim 1, wherein the information received at said second computer has different but related content as the information sent from said first computer. (MacTB, Chapter 1, see page 1-1)

For claim 11, MacTB teaches, the system according to claim 1, further comprising: at least a third computer, wherein at least said third computer receives information from said first server related to the information sent from said first computer, wherein at least said third computer is separated from said communication network by at least one of said first or at least a second firewall. (MacTB, Chapter 1, see images and page 1-3, firewall)

For claim 12, MacTB teaches, the system according to claim 1, wherein a communication pathway between said first server and at least one of said first computer and said second computer is kept open by repeated transmissions from said first server. (MacTB, Chapter 3, see page 3-17, time out setting)

For claim 13, MacTB teaches, the system according to claim 1, wherein a communication pathway between said first server and at least one of said first computer

and said second computer is kept open by repeated transmissions from at least one of said first computer and said second computer. (MacTB, Chapter 3, see page 3-17, time out)

For claim 15, MacTB teaches, the system according to claim 1, wherein said first computer transmits a said message to said first server with a header, the header including at least one of an encrypted header, an encrypted identification, an encrypted IP address, an encrypted username of said second computer, an encrypted size, an encrypted CRC, an encrypted header length, an encrypted message length, an encrypted asset identifier, an encrypted name of at least one client, and an encrypted application ID, an encrypted time and date stamp, an encrypted location ID, an encrypted message types, an encrypted attachment identifier, an encrypted packet number, and an encrypted pre-compressed data size for an associated message. (MacTB, Chapter 1, see page 1-1, the whole message is encrypted and encapulated)

For claim 19, MacTB teaches, a method for transmitting information across a network comprising the steps of:

receiving an encrypted identification of a second computer from a first computer; (MacTB, Chapter 1, the whole message is encrypted and encapsulated)

receiving an encrypted message from said first computer; (MacTB, Chapter 1, the whole message is encrypted and encapsulated)

decrypting said encrypted identification into an unencrypted identification of said second computer; and, (MacTB, Chapter 1, the whole message is encrypted and encapsulated, which is de-encapsulated and decrypted at the PPTP/L2TP server)

transmitting said encrypted message to said second computer, wherein at least one of said receiving steps and said transmitting step includes receiving or transmitting through a firewall. (MacTB, Chapter 1, PPTP/L2TP server is behind the firewall)

For claim 20, MacTB teaches, the method according to claim 19, wherein said encrypted message is also compressed. (MacTB, Chapter 1, see page 1-1)

For claim 21, WinTB-MacTB teaches, a computer-readable medium storing a program for transmitting information across a network, said program comprising the steps of:

receiving an encrypted identification of a second computer from a first computer; (MacTB, Chapter 1, RC-4 encryption)

receiving an encrypted message from said first computer; decrypting said encrypted identification into an unencrypted identification of said second computer; (MacTB, Chapter 1, unencrypted at PPTP/L2TP server, remove from encapsulation, with ip address)

and transmitting said encrypted message to said second computer, without decrypting said encrypted message (MacTB, Chapter 1, it is inherent to internet to transmit without decrypting, since the message is encapsulated)

wherein at least one of said receiving steps and said transmitting step includes receiving or transmitting through a firewall port that is normally open by default to Internet traffic. (see applicant's specification "generally open" in paragraph 4 of the specification) (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 21.

For claim 22, MacTB teaches, the computer readable medium according to claim 21, wherein said encrypted message is also compressed. (MacTB, Chapter 1, see page 1-1)

For claim 24, MacTB teaches, a method for transmitting information across a network comprising the steps of:

encrypting an identification of a second computer at a first computer; (MacTB, Chapter 1, encapsulated message in PPTP/L2TP)

encrypting a message such that said message can only be decrypted by said second computer; and (MacTB, Chapter 1, RC-4)

transmitting to a server said encrypted identification and said encrypted message, wherein said server later decrypts said encrypted identification and transmits said encrypted message to said second computer, (MacTB, Chapter 1, keys and PPTP/L2TP)

wherein at least one of said first computer and said second computer are separated from a server by a firewall. (MacTB, Chapter 1, see pages 1-1 and 1-3, also see images, firewall)

For claim 26, WinTB-MacTB teaches, a computer readable medium storing a program for transmitting information across a network, said program comprising the steps of:

encrypting an identification of a second computer at a first computer; (MacTB, Chapter 1, RC-4, encapsulated message in PPTP/L2TP)

encrypting a message such that said message can only be decrypted by said second computer; and (MacTB, Chapter 1, RC-4, keys)

transmitting to a server said encrypted identification and said encrypted message, wherein said server later decrypts said encrypted identification and transmits said encrypted message to said second computer, (MacTB, Chapter 1, decrypted at PPTP/L2TP server and forwarded)

wherein at least one of said first computer and said second computer are separated from said server by a firewall and wherein said encrypted message is transmitted through a port on the firewall that is normally open by default to Internet traffice. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images, firewall) (see applicant's specification "generally open" in paragraph 4 of the specification) (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 26.

For claim 27, WinTB-MacTB teaches, a system for transmitting information between a first computer and a second computer comprising:

a first application; (MacTB, Chapter 1, internet, website)

a first computer hosting a first client, said first client receiving data from said first application, said first computer transmitting said data to a server, said server forwarding said data to a second client residing on said second computer, said second client forwarding said data to at least a second application, (MacTB, Chapter 1, PPTP/L2TP, forward from server)

wherein at least one of said first computer and said second computer are separated from said server by a firewall, (MacTB, Chapter 1, firewall)

wherein said first computer transmits a message to said server with an encrypted identification of said second computer said message bein encrypted for decryption at said second computer (MacTB, Chapter 1, RC-4, keys) and

wherein said server decrypts said encrypted identification to an unencrypted identification of said second computer and forwards said message to said second computer using said unencrypted identification(MacTB, Chapter 1, PPTP/L2TP forwards unencrypted, decapulated message)

wherein one of said encrypted message transmitted from said first computer and said encrypted message forwarded to said second computer are transmitted through a firewall port that is normally one by default to Internet traffic. (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) (see applicant's specification "generally open" in paragraph 4 of the specification)The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 27.

For claim 28, MacTB teaches, the system according to claim 27, wherein said first application is hosted by a third computer that communicates with said first computer. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images, see computer network, server)

For claim 29, MacTB teaches, the system according to claim 27, wherein said first application is hosted by said first computer. (MacTB, Chapter 1, see page 1-1 and 1-3, internet)

For claim 30, MacTB teaches, the system according to claim 27, wherein said second application is hosted by a third computer that communicates with said second computer. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images, server)

For claim 31, MacTB teaches, the system according to claim 27, wherein said second application is hosted by said second computer. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images)

For claim 32, MacTB teaches, the system according to claim 27, wherein said first computer transmits said data as encrypted data and said server transmits said encrypted data to said second computer. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images, internet)

For claim 34, WinTB-MacTV teaches, the system according to claim 27, wherein said first computer and said second computer each use an open port to access to said communications network. (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80)The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 34.

For claim 35, WinTB-MacTB teaches, the system according to claim 34, wherein said open port is at least one of port 80 and port 8080. (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 35.

For claim 36, MacTB teaches, the system according to claim 27, wherein said first client communicates with said first application by an application programming interface. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images, internet website)

For claim 37, MacTB teaches, the system according to claim 27, wherein said first client communicates with said first application by a proxy. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images, PPTP/L2TP becomes a proxy, because it directs internet back to remote client)

For claim 38, MacTB teaches, the system according to claim 27, wherein said first client communicates with said first application by sockets. (MacTB, Chapter 1, see page 1-1 and 1-3, also see images, internet is sockets)

For claim 45, WinTB-MacTB teaches, a computer readable medium storing a program for transmitting information across a network between a first computer and a second computer, said network including a server that has received an decrypted an encrypted identification of said second computer, (MacTB, Chapter 1, PPTP/L2TP server)

said server having transmitted an encrypted identification of said second computer, said server having transmitted and encrypted message to said second computer using said decrypted identification said encrypted message having been encrypted at said first computer for decrypting at said second computer, (MacTB, Chapter 1, RC-4, keys)

said program comprising the steps of:

receiving at said second computer from a server said encrypted massage and a header with encrypted information(MacTB, Chapter 1, encapsulated message form PPTP/L2TP message)

decrypting said encrypted information; (MacTB, Chapter 1, PPTP/L2TP server)

decrypting said encrypted message, (MacTB, Chapter 1, PPTP/L2TP server0

and wherein at least one of said first computer and said second computer are separated from said server by a firewall and said encrypted message is transmitted through firewall port that is normally open by default to Internet traffic. (MacTB, Chapter 1, see page 1-1 and 1-3, firewall) (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) (see applicant's specification "generally open" in paragraph 4 of the specification)The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 45.

For claim 46, MacTB teaches, the computer readable medium according to claim 45,

wherein said header includes at least one of an encrypted identification, an encrypted IP address, an encrypted username of said second computer, an encrypted size, an encrypted CRC, an encrypted header length, an encrypted message length, an encrypted asset identifier, an encrypted name of at least one client, and an encrypted application ID, an encrypted time and date stamp, an encrypted location ID, an encrypted message types, an encrypted attachment identifier, an encrypted packet

number, and an encrypted pre-compressed data size for an associated message. (MacTB, Chapter 1, see page 1-1 and 1-3, whole message is encapsulated and encrypted)

For claim 47, WinTB-MacTB teaches, a method of transferring data between a first computer and a second computer coupled over a network, comprising the step of:

(1) receiving a first hypertext transfer protocol (HTTP) message contained information intended for delivery to the second computer, wherein the first message is received through a first firewall associated with the first computer thought a port that is normally open y default to Internet traffic. (MacTB, Chapter 1, see page 1-1 and 1-3, firewall, PPTP/L2TP tunnel establishment message) (see www.nts.com website, Firewalls a problem? Looks like a job for … SuperTunnel!, port 80) (see applicant's specification "generally open" in paragraph 4 of the specification)

(2) receiving a second hypertext transfer protocol (HTTP) message from the second computer, wherein the second message causes a return path to be established to the second firewall associated with the second computer that is normally open by default to Internet traffice; and(see www.nts.com website, Firewalls a problem? Looks like a job for … SuperTunnel!, port 80) (MacTB, Chapter 1, see page 1-1 and 1-3, firewall, PPTP/L2TP tunnel establishment message)

(3) transmitting to the second computer via the return path contents of the first message received from the first computer (MacTB, Chapter 1, path is constant, through the firewall and PPTP/L2TP server)

The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 47.

For claim 48, the method of claim 47, wherein the first and second HTTP message each comprise a HTTP POST message. It would have been obvious to on of ordinary skill in the art at the time of the invention was made to make use of HTTP POST message because it provided for sending back information to create a connection that would normally be sent over port 80, since any other message type would be unexpected.

For claim 49, MacTB, the method of claim 47 wherein steps (1) through (3) are preformed on an intermediate server computer that is separated for the first computer and the second computer. (MacTB, Chapter 1, see page 1-1 and 1-3, firewall, PPTP/L2TP server)

For claim 50, MacTB teaches, the method of claim 49 wherein steps (1). The first message received from the first computer is encrypted by the first computer, and wherein the step (3) the third computer transmits encrypted message content received

form the first computer to the second computer via the return path. (MacTB, Chapter 1, see page 1-1 and 1-3, firewall, PPTP/L2TP server)

For claim 51, MacTB, teaches, the method of claim 50, wherein the intermediate server computer decrypts at least a portion of the first message using a first encryption key common between the first and third computer to create and unencrypted portion, and then re-encrypts the unencrypted portion using a second encryption key common between the second and third computer, wherein the first and second encryption keys are different. It is obvious of one of ordinary skill in the art to duplicate the system multiple times. (MacTB, Chapter 1, see page 1-1 and 1-3, firewall, PPTP/L2TP server)

For claim 52, WinTB- MacTB, teaches, the method of claim 47, further comprising the step of:

(4) receiving a third HTTP message contained information intended for delivery to the first computer, wherein the third message is received through the firewall associated with the second computer throught port hat is normally open by default to Ineternet traffic; and(MacTB, Chapter 1, see page 1-1 and 1-3, firewall, PPTP/L2TP tunnel establishment message) (see www.nts.com website, Firewalls a problem? Looks like a job for ... SuperTunnel!, port 80) (see applicant's specification "generally open" in paragraph 4 of the specification)

(5) transmitting content of the third message to the first computer over a return path previously established between the first computer and the third computer. (MacTB, Chapter 1, tunnel is setup so path remains the same)

The same motivation that was utilized in the rejection of claim 1, applies equally as well to claim 51.

For claim 53, MacTB teaches, the method of claim 47, further comprising the steps of when no message been received for the first computer for delivery to the second computer, periodically transmitting to the second computer via the return path a message to avoid a time-out condition on the second computer. (MacTB, Chapter 1, 3-17)

For claim 54, MacTB teaches, the method of claim 47, further comprising the step of authenticating that the first computer is authorized to communicated with the second computer prior to step (3). (MacTB, Chapter 1, keys are prior authoriziaton)

Claims 55-56 list all the same elements of claims 47-54. Therefore, the supporting rationale of the rejection to claims 47-54 applies equally as well to claims 55-56.

Claims 6, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of TunnelBuilder for Mac User's Guide in view of TunnelBuilder 4.01 for

Windows Website (referred to as WinTB) and van der Sijpt (U.S. Patent 5,802,293).

For claim 6, MacTB-WinTB fails to teaches, the system according to claim 1, further comprising a second server that operates in the event of an error with said first server.

Van der Sijpt teaches, the system according to claim 1, further comprising a second server that operates in the event of an error with said first server. (see van der Sijpt, Col. 16 lines 25-35)

It would have been obvious to on of ordinary skill in the art at the time of the invention was made to combine the system disclose in TunnelBuilder for Mac with the method of van der Sijpt since both invention are from analogous art of communication between computer on a network. (MacTB, Chapter 1, also see images) and (see van der Sijpt, Col. 2 lines 45-63)

For claim 9, MacTB-WinTB-van der Sijpt teaches, the system according to claim 1, further comprising a second server, said second server being connected to said network, wherein said second server replaces said first server when an error occurs between said first server and at least one of said first computer and said second computer. (see van der Sijpt, Col. 16 lines 25-35)

The same motivation that was utilized in the rejection of claim 6, applies equally as well to claim 9.

For claim 10, MacTB-WinTB -van der Sijpt teaches, the system according to claim 1, further comprising a second server, said second server being connected to said network, wherein said second server replaces said first server when an error occurs with said first server. (see van der Sijpt, Col. 16 lines 25-35)

The same motivation that was utilized in the rejection of claim 6, applies equally as well to claim 10.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ajay M. Bhatia whose telephone number is (571)-272-3906. The examiner can normally be reached on M-F 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jason Cardone can be reached on (571)272-3933. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AB

SALEH NAJJAR
SUPERVISORY PATENT EXAMINER